

# Configurações de Segurança para o Apple iOS 9

Carlos Henrique G. de Araújo

6 de abril de 2016

# Sumário

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Introdução</b>  | <b>3</b>  |
| <b>2</b> | <b>Interface do Usuário</b>  | <b>5</b>  |
| 2.1      | Atualizar o dispositivo para a versão mais recente do iOS . . . . .                  | 5         |
| 2.2      | Habilitar o bloqueio do dispositivo através de código . . . . .                      | 6         |
| 2.3      | Configurar o modo de espera da tela . . . . .  | 6         |
| 2.4      | Desativar o recurso de VPN . . . . .   | 6         |
| 2.5      | Desativar o Bluetooth . . . . .  | 7         |
| 2.6      | Desativar o AirDrop . . . . .  | 7         |
| 2.7      | Desativar as solicitações de conexão a redes Wi-Fi . . . . .                         | 7         |
| 2.8      | Habilitar o download automático de atualizações de aplicativos . . . . .             | 8         |
| 2.9      | Apagar as informações armazenadas no dispositivo antes de se desfazer dele . . . . . | 8         |
| <b>3</b> | <b>Configurações avançadas</b>   | <b>10</b> |
| 3.1      | Desabilitar o uso de códigos de desbloqueio simples . . . . .                        | 10        |
| 3.2      | Habilitar a eliminação de informações . . . . .                                      | 10        |
| 3.3      | Desativar o desbloqueio através do Touch ID . . . . .                                | 11        |
| 3.4      | Desabilitar o acesso à Central de Controle a partir da tela bloqueada . . . . .      | 11        |
| 3.5      | “Esquecer” redes Wi-Fi . . . . .   | 12        |
| 3.6      | Desabilitar todo o recurso de redes Wi-Fi . . . . .                                  | 12        |
| 3.7      | Desabilitar o Acesso Pessoal . . . . .   | 12        |
| 3.8      | Desabilitar o serviço de localização . . . . .                                       | 13        |
| 3.9      | Habilitar o Modo Avião . . . . .   | 13        |
| 3.10     | Não exibir notificações de aplicativos na tela bloqueada . . . . .                   | 14        |
| 3.11     | Habilitar o recurso Buscar iPhone (ou Buscar iPad) . . . . .                         | 14        |
| 3.12     | Habilitar uma senha para acesso ao cartão SIM . . . . .                              | 14        |
| <b>4</b> | <b>Configurações para o navegador Safari</b>   | <b>16</b> |
| 4.1      | Desabilitar a execução de código Javascript . . . . .                                | 17        |
| 4.2      | Habilitar o aviso de websites fraudulentos . . . . .                                 | 17        |
| 4.3      | Desabilitar o preenchimento automático de informações de contato . . . . .           | 17        |
| 4.4      | Desabilitar preenchimento automático de nomes e senhas . . . . .                     | 18        |
| 4.5      | Desabilitar o preenchimento automático de cartões de crédito . . . . .               | 18        |
| 4.6      | Apagar informações sobre senhas armazenadas . . . . .                                | 18        |
| 4.7      | Remover informações armazenadas sobre cartões de crédito . . . . .                   | 19        |
| 4.8      | Habilitar a navegação privada . . . . .  | 19        |
| 4.9      | Impedir o rastreamento durante a navegação . . . . .                                 | 20        |



# Prefácio

O iOS (anteriormente conhecido como iPhone OS) é um sistema operacional desenvolvido pela Apple para os dispositivos móveis da própria empresa, como iPhones, iPads, e iPod Touch. É o segundo sistema operacional móvel mais popular do mundo, atrás apenas do sistema Android.

Este pequeno livro detalha um conjunto de recomendações que visam tornar o sistema operacional iOS mais seguro contra acesso indevido, vazamento de informações confidenciais, etc. A versão do sistema operacional iOS que será tratada aqui é a 9.3.

Este trabalho foi originalmente concebido para ser lido pelo maior número de pessoas possível, como administradores de sistemas, analistas de segurança, ou simplesmente usuários finais curiosos e entusiastas da área de segurança ou do sistema operacional iOS.

O livro é composto por quatro capítulos, que vão das recomendações básicas até as mais avançadas. Cabe aqui uma breve definição desta categorização.

As recomendações básicas são práticas e prudentes, fornecem um claro benefício em relação à segurança, e geram um impacto mínimo na usabilidade do dispositivo iOS. Já as recomendações avançadas destinam-se a dispositivos iOS nos quais a segurança é primordial, atuam em sua maioria como medidas de defesa em profundidade, e podem impactar significativamente a usabilidade do dispositivo.

Em cada capítulo, as recomendações de segurança são apresentadas textualmente, e separadas em itens. Cada item é composto por:

- um título
- uma breve descrição, detalhando o item e seu propósito
- instruções detalhadas, explicando como realizar a configuração a fim de que o propósito do item seja alcançado

## Por que L<sup>A</sup>T<sub>E</sub>X?

Caso o leitor tenha visualizado os arquivos utilizados para se criar este documento, terá percebido que eles não foram escritos em Word, LibreOffice, ou HTML. Eles foram escritos utilizando-se o L<sup>A</sup>T<sub>E</sub>X.

Para quem não conhece, o L<sup>A</sup>T<sub>E</sub>X (Lamport TeX) é um processador de textos e uma linguagem de marcação de documentos criado por um cientista da computação americano chamado Leslie Lamport. Ele se baseou em um outro processador de textos, chamado TeX, este criado por um cientista da computação americano chamado Donald Knuth.

Inicialmente criado para a elaboração de textos acadêmicos da área de ciências exatas, hoje em dia o L<sup>A</sup>T<sub>E</sub>X é usado na área econômica e até política.

Decidiu-se escrever este trabalho em  $\text{\LaTeX}$  devido a algumas vantagens que ele oferece, tais como:

- textos em  $\text{\LaTeX}$  são escritos em texto plano, mas a ferramenta possui compiladores de conversão para diversos outros formatos: DVI, PDF, HTML, RTF, etc.
- ele possui suporte à modularização do texto, o que permite escrever capítulos e seções em arquivos fisicamente separados
- pode-se editar textos escritos em  $\text{\LaTeX}$  em diversos softwares, desde o vim (Linux) até o TeX-nicCenter (Windows)
- não importa qual a plataforma (Windows, Linux, Mac OS, etc.) utilizada, o texto resultante será sempre o mesmo

Existem, porém, algumas situações em que o usar o  $\text{\LaTeX}$  pode se tornar desvantajoso. Para escrever documentos que necessitam de recursos visuais mais sofisticados, por exemplo, talvez o  $\text{\LaTeX}$  não seja a melhor opção.

# Capítulo 1

## Introdução

Este capítulo tem o objetivo de definir algumas premissas básicas, antes de se iniciar com as recomendações de segurança. A primeira delas é que o sistema operacional iOS pode ser encontrado em uma gama diversa de aparelhos, como iPhones, iPads, e o iPod Touch. Por isso, com o objetivo de simplificar a nomenclatura utilizada, tais equipamentos serão referenciados daqui por diante como dispositivos iOS.

Todas as recomendações aqui descritas foram testadas em um iPad de quarta geração e em um iPhone 5s. As instruções das recomendações de segurança foram criadas com base na interface de usuário destes dispositivos. No caso deles, todas recomendações listadas quase sempre têm início pressionando o ícone Ajustes. Segue abaixo a localização deste ícone.




Figura 1.1: O ícone Ajustes, destacado em vermelho

É necessário enfatizar que estas recomendações tratam da versão 9.3 do iOS. O leitor pode verificar se esta é a versão presente em seu dispositivo seguindo as instruções logo abaixo.

1. Pressionar o ícone Ajustes
2. Pressionar Geral
3. Pressionar Sobre

4. Verificar se o valor de Versão é 9.3 ou superior



|                 |                   |
|-----------------|-------------------|
| Aplicativos     | 51                |
| Capacidade      | 12,5 GB           |
| Disponível      | 2,0 GB            |
| Versão          | 9.3 (13E233)      |
| Modelo          | MD510LL/A         |
| Número de Série | DMPKC7NKF182      |
| Wi-Fi           | 60:FE:C5:81:6F:10 |
| Bluetooth       | 60:FE:C5:81:6F:11 |

Figura 1.2: A versão presente no dispositivo usado para testes, destacada em vermelho

Vale lembrar que o autor não se responsabiliza por eventuais danos causados em dispositivos iOS decorrentes da aplicação das configurações recomendadas aqui. Por isso, é sugerido que, se possível, estas recomendações sejam aplicadas inicialmente em aparelhos de teste para, apenas depois, serem aplicadas em outros dispositivos.

Realizar backups das informações contidas no dispositivo também é uma prática recomendável para a recuperação de informações importantes, caso ocorram eventuais problemas. Seguem logo abaixo instruções para a realização de backups em dispositivos iOS:

1. Pressionar o ícone Ajustes
2. Pressionar iCloud
3. Selecionar para backup todas as informações que o usuário considerar importantes (E-mail, Contatos, etc.)
4. Pressionar Backup
5. Na tela seguinte, ativar Backup do iCloud deslizando o controle para a direita
6. Na mesma tela, caso o usuário esteja conectado a uma rede Wi-Fi, pressionar Efetuar Backup Agora

# Capítulo 2

## Interface do Usuário

Este capítulo concentra recomendações de segurança que dizem respeito à interface do usuário. Como mencionado no prefácio, estas recomendações possuem como características, serem práticas e prudentes, fornecerem um claro benefício em relação à segurança, e gerarem um impacto mínimo na usabilidade do dispositivo iOS.

### 2.1 Atualizar o dispositivo para a versão mais recente do iOS

Seguir esta recomendação garante que a versão do sistema operacional iOS instalada no dispositivo seja sempre a mais recente. As versões atualizadas geralmente trazem consigo correções para falhas críticas de segurança.

Assim, manter o sistema iOS sempre atualizado reduz a probabilidade de pessoas mal intencionadas e com competência técnica, explorarem remotamente vulnerabilidades presentes no dispositivo.

Há duas maneiras de se verificar atualizações do iOS estão disponíveis. Via OTA (over-the-air), ou através do iTunes. Caso o leitor queira verificar atualizações via OTA, deve-se fazer o seguinte:

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar Atualização de Software
4. Caso alguma atualização esteja disponível, pressionar Download
5. Após o download, pressionar Instalar, para atualizar o iOS

Caso o leitor queira verificar atualizações através do iTunes, deve-se fazer o seguinte:

1. Conectar o dispositivo ao computador
2. Abrir o iTunes
3. Na lista de dispositivos, selecionar o dispositivo a ser atualizado
4. Clicar em Verificar Atualizações



5. Caso haja alguma atualização disponível, clicar em Baixar e Instalar

É bom lembrar que não se deve desligar nem desconectar o dispositivo (no caso da atualização via iTunes) enquanto o processo de atualização não terminar!

## 2.2 Habilitar o bloqueio do dispositivo através de código

Esta recomendação determina que um código de bloqueio seja sempre solicitado antes de se permitir o acesso ao dispositivo.

É altamente recomendado que um código de bloqueio seja configurado, para que pessoas estranhas não adquiram acesso fácil e imediato às informações armazenadas no dispositivo.

1. Pressionar Ajustes
2. Pressionar Código ou Touch ID e Código
3. Pressionar Ativar Código
4. Digitar um código
5. Digitar novamente o código

## 2.3 Configurar o modo de espera da tela

Esta recomendação define a quantidade de minutos em que o dispositivo pode ficar inativo antes de requerer a senha novamente. Claro que, quanto menor o tempo, menor será a probabilidade de pessoas mal intencionadas acessarem informações sem a necessidade de se digitar uma senha. O tempo recomendado é de dois minutos.

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar Bloqueio automático
4. Selecionar 2 minutos

## 2.4 Desativar o recurso de VPN

Dispositivos iOS podem se conectar nativamente a serviços de VPN que usam os seguintes protocolos:

- L2TP sobre IPSec
- PPTP
- IPSec da Cisco

Caso o dispositivo possua uma conexão VPN configurada, ele só deve ser ativado quando for necessário. Do contrário, aplicativos maliciosos ou “trojanizados”, podem acessar os recursos de VPN do dispositivo.

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar VPN
4. Desativar o recurso de VPN, caso ele esteja ativado

## 2.5 Desativar o Bluetooth

A tecnologia Bluetooth permite a conexão de diversos acessórios ao dispositivo (fones de ouvido, kits veiculares, teclados, e outros) sem a necessidade de fios.

É recomendado que tal recurso permaneça desativado quando não estiver em uso, caso contrário haverá um aumento do risco de descoberta do dispositivo e de conexão a serviços desconhecidos e não confiáveis baseados nesta tecnologia.

1. Pressionar Ajustes
2. Pressionar Bluetooth
3. Desativar o Bluetooth, caso ele se encontre ativado

## 2.6 Desativar o AirDrop

Esta configuração evita que o dispositivo seja descoberto, via Airdrop, por alguém (incluindo os contatos).

A justificativa para a sua desativação é a mesma do caso do Bluetooth, na seção anterior.

1. Desbloquear o dispositivo
2. Deslizar a parte inferior da tela para cima, a fim de exibir a Central de Controle
3. Pressionar o campo AirDrop na parte inferior da Central de Controle
4. Pressionar Inativo

## 2.7 Desativar as solicitações de conexão a redes Wi-Fi

Quando o dispositivo (seja ele um iPhone, um iPad, ou um iPod) tenta se conectar à internet mas não está em uma faixa de redes Wi-Fi previamente utilizada, ele procura por outras redes e exibe uma lista de todas as redes Wi-Fi disponíveis, para que o usuário escolha alguma.

É recomendado que tal funcionalidade seja desativada. O usuário terá de configurar e se conectar manualmente a uma rede Wi-Fi, mas este comportamento reduz as chances de se conectar inadvertidamente a redes não confiáveis.

1. Pressionar Ajustes
2. Pressionar Wi-Fi
3. Desativar a opção Solicitar Conexão

## 2.8 Habilitar o download automático de atualizações de aplicativos

Esta recomendação garante que as versões dos aplicativos instalados no dispositivo sejam sempre as mais recentes.

A justificativa é que as versões mais recentes geralmente trazem consigo correções para falhas críticas de segurança.

1. Pressionar Ajustes
2. Pressionar iTunes Store e App Store
3. Na seção TRANSFERÊNCIAS AUTOMÁTICAS, ativar a opção Atualizações

## 2.9 Apagar as informações armazenadas no dispositivo antes de se desfazer dele

Recomenda-se apagar todas as informações contidas no armazenamento interno do dispositivo, restaurando-o para as configurações padrões de fábrica, antes de se desfazer dele.

Algumas situações incluem:

- entregar o aparelho para a assistência técnica, para conserto
- vendê-lo para outra pessoa
- doá-lo a alguém
- jogá-lo diretamente no lixo

Manter informações pessoais no dispositivo antes de repassá-lo, aumenta o risco de pessoas maliciosas acessarem e publicarem informações confidenciais armazenadas. Esta tem sido uma das principais causas de vazamentos de fotos e vídeos íntimos na internet.

Realizar cópias de segurança (backups) das informações, antes de se realizar a remoção das mesmas, também é importante.

Antes de se restaurar o dispositivo para as configurações de fábrica, é necessário desativar o serviço iMessage, procedendo da seguinte forma:

1. Pressionar Ajustes
2. Pressionar Mensagens
3. Desativar o iMessage

E finalmente, seguem logo abaixo as instruções para se restaurar o dispositivo, apagando quaisquer informações pessoais armazenadas:

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar Redefinir
4. Pressionar Redefinir Todos os Ajustes
5. Digitar o código, caso o mesmo tenha sido previamente configurado

# Capítulo 3

## Configurações avançadas

Este capítulo também concentra recomendações de segurança que dizem respeito à interface do usuário. Porém, devido às suas características peculiares, destinam-se a dispositivos iOS nos quais a segurança é primordial. Estas recomendações podem impactar significativamente a usabilidade do dispositivo, por isso é recomendado considerá-las como medidas de defesa em profundidade.

### 3.1 Desabilitar o uso de códigos de desbloqueio simples

Esta recomendação determina que códigos de bloqueio de apenas quatro dígitos não sejam permitidos para se proteger o acesso ao dispositivo. É recomendado que o dispositivo seja configurado para permitir o uso de códigos de bloqueio com mais de quatro caracteres alfanuméricos (números, letras, símbolos, etc).

Permitir uma senha alfanumérica para desbloquear o dispositivo iOS aumenta a dificuldade que uma pessoa mal intencionada terá na tentativa de realizar acessos não autorizados.

1. Pressionar Ajustes
2. Pressionar Código, ou Touch ID e Código
3. Pressionar Alterar Código, ou Ativar Código
4. Caso algum código já tenha sido configurado, será necessário digitá-lo
5. Pressionar Opções de código
6. Pressionar Código Alfanumérico Personalizado
7. Digitar um código alfanumérico e pressionar Seguinte
8. Digitar novamente o código alfanumérico e pressionar OK

### 3.2 Habilitar a eliminação de informações

Esta configuração determina que o dispositivo iOS apague todo o seu conteúdo (vídeos, fotos, etc) após dez tentativas fracassadas de desbloqueio.

Sucessivas tentativas fracassadas de desbloqueio do aparelho sugerem que ele não se encontra nas mãos de seu proprietário. Neste caso, apagar todo o conteúdo garante a confidencialidade das informações armazenadas no dispositivo.

1. Pressionar Ajustes
2. Pressionar Código, ou Touch ID e Código
3. Pressionar Alterar Código, ou Ativar Código
4. Caso algum código já tenha sido configurado, será necessário digitá-lo
5. Ativar a opção Eliminar Dados

### 3.3 Desativar o desbloqueio através do Touch ID

O Touch ID permite o uso de uma ou mais impressões digitais como código de desbloqueio, através de um simples toque do botão Home. O sensor do Touch ID “lê” a impressão digital e automaticamente desbloqueia o telefone.

Desabilitar este recurso evita o risco de uma autenticação não autorizada via Touch ID, seja através de falsos positivos, seja através de ataques intencionais.

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar Código, ou Touch ID e Código
4. Caso algum código já tenha sido configurado, será necessário digitá-lo
5. Desativar a opção Desbloquear iPhone, ou Desbloquear iPad

Vale lembrar que esta configuração se aplica apenas a dispositivos iOS mais recentes.

### 3.4 Desabilitar o acesso à Central de Controle a partir da tela bloqueada

Ao longo da história do sistema iOS, já foram descobertas algumas maneiras de se contornar a proteção da tela bloqueada. Esta recomendação desabilita o acesso à Central de Controle a partir da tela.

A ideia aqui é eliminar a possibilidade de a Central de Controle vir ser usada como um meio para se contornar a proteção da tela bloqueada.

1. Pressionar Ajustes
2. Pressionar Central de Controle
3. Desativar a opção Acesso na Tela Bloqueada

### 3.5 “Esquecer” redes Wi-Fi

Esta configuração faz com que o dispositivo iOS “esqueça” redes Wi-Fi nas quais ele já tenha conectado.

Uma rede Wi-Fi confiável, mas sem autenticação, pode ser mascarada e o dispositivo pode se conectar automaticamente a ela se a mesma não tiver sido “esquecida” pelo dispositivo desde a última conexão.

Outra situação possível é quando a rede Wi-Fi mantém seu nome padrão, de fábrica, e o dispositivo iOS encontra uma outra rede não confiável de mesmo nome e acabe tentando se conectar a ela automaticamente.

Para esta recomendação, é necessário que o Wi-Fi esteja ativado e a rede Wi-Fi a ser esquecida esteja próxima ao dispositivo.

1. Pressionar Ajustes
2. Pressionar Wi-Fi
3. Na lista ESCOLHA UMA REDE..., localizar a rede a ser esquecida e pressionar o símbolo de exclamação.
4. Na tela seguinte, pressionar Esquecer Esta Rede
5. Confirmar o esquecimento da rede

### 3.6 Desabilitar todo o recurso de redes Wi-Fi

Em ambientes onde a segurança é prioridade, recomenda-se que o recurso de conexão a redes Wi-Fi permaneça desabilitado no dispositivo Android. Caso ele possua acesso a serviços de dados celulares (3G ou 4G por exemplo), a conexão à internet deverá ocorrer através destas redes.

1. Pressionar Ajustes
2. Pressionar Wi-Fi
3. Desativar a Wi-Fi

### 3.7 Desabilitar o Acesso Pessoal

O Acesso Pessoal permite que o usuário compartilhe sua conexão à internet, via 3G ou 4G, com outros dispositivos, através de Wi-Fi, Bluetooth, ou cabo USB.

Desabilitar o Acesso Pessoal, quando o mesmo não é necessário, elimina a possibilidade de o recurso vir a ser usado como um meio para que pessoas mal intencionadas tecnicamente preparadas ataquem remotamente o dispositivo iOS.

1. Pressionar Ajustes
2. Pressionar Acesso Pessoal
3. Desativar o Acesso Pessoal, caso ele se encontre ativado

### 3.8 Desabilitar o serviço de localização

O serviço de localização permite que alguns aplicativos instalados no dispositivo iOS obtenham e usem informações que indiquem a localização física do usuário. Esta localização é determinada através do GPS do dispositivo, da rede celular 3G ou 4G, e de redes Wi-Fi. Se o usuário desativar os serviços de localização, ele receberá do solicitações para reativá-la, sempre que algum aplicativo quiser fazer uso deste recurso.

Manter o serviço de localização ativado aumenta a capacidade de pessoas mal intencionadas, com considerável conhecimento técnico, rastreamento a localização do usuário através de sites web, aplicativos, etc.

1. Pressionar Ajustes
2. Pressionar Privacidade
3. Pressionar Serv. Localização
4. Na tela seguinte, desativar o serviço de localização

### 3.9 Habilitar o Modo Avião

Quando está habilitado, o Modo Avião desativa todos os transmissores e receptores de sinais de rádio do dispositivo iOS. Alguns serviços desativados, são:

- Envio e recebimento de ligações
- Envio e recebimento de SMS e MMS
- Dados móveis (3G, 4G)
- GPS
- Wi-Fi
- Bluetooth

Assim, quando estas funcionalidades forem desnecessárias, é recomendado manter o dispositivo no Modo Avião. Caso a transmissão e recepção de sinais permaneçam habilitados mesmo sem necessidade, haverá um aumento da possibilidade de que estes sinais de rádio sejam usados como um meio para se atacar remotamente o dispositivo.

1. Pressionar Ajustes
2. Ativar o Modo avião



### 3.10 Não exibir notificações de aplicativos na tela bloqueada

Esta configuração previne que notificações oriundas de aplicativos instalados sejam exibidas quando o dispositivo iOS encontra-se bloqueado.

É recomendado que tal visualização seja desabilitada para todos os aplicativos nos quais é desejada confidencialidade. Do contrário, pessoas que não possuem o código de desbloqueio poderão visualizar notificações, aumentando assim o risco de vazamento de informações importantes.

1. Pressionar Ajustes
2. Pressionar Notificações
3. Na lista ESTILO DA NOTIFICAÇÃO, localizar o aplicativo e pressioná-lo
4. Na tela seguinte, desativar a opção Mostrar na Tela Bloqueada
5. Repetir os passos 3 e 4 para outros aplicativos

### 3.11 Habilitar o recurso Buscar iPhone (ou Buscar iPad)

Esta configuração habilita as seguintes funcionalidades no dispositivo iOS:

- o rastreamento remoto da localização do dispositivo
- a eliminação remota de informações armazenadas no dispositivo
- a exibição remota de mensagens

Habilitar o recurso Buscar iPhone (ou Buscar iPad) no iOS ativa a capacidade de se localizar o dispositivo através do aplicativo iOS Buscar iPhone, ou através do site do iCloud. Também exibe uma mensagem personalizada com um número de telefone à sua escolha na tela bloqueada, e previne a execução de ações importantes sem a digitação da senha do Apple ID, como a eliminação das informações armazenadas no dispositivo iOS e sua configuração.

1. Pressionar Ajustes
2. Pressionar iCloud
3. Pressionar Buscar iPhone (ou Buscar iPad)
4. Na tela seguinte, ativar a opção Buscar iPhone (ou Buscar iPad)

### 3.12 Habilitar uma senha para acesso ao cartão SIM

O cartão SIM, conhecido como chip da operadora de telefonia celular, permite a realização de ligações telefônicas, além do armazenamento de informações de contatos, e de outras informações pessoais. Este controle assegura que o cartão SIM, caso seja perdido ou roubado, não será usado em nenhum outro dispositivo.

Uma pessoa com intenções maliciosas pode retirar o cartão SIM de um telefone e inseri-lo em outro telefone, realizar ligações, enviar mensagens, etc. Adicionar uma senha ao cartão protegerá contra este tipo de ataque. Tal senha será requisitada pelo dispositivo sempre que o cartão SIM for acessado.

1. Pressionar Ajustes
2. Pressionar Telefone
3. Pressionar PIN do SIM
4. Digitar um PIN

## Capítulo 4

# Configurações para o navegador Safari

Este capítulo traz recomendações de segurança que dizem respeito ao Safari, que é o navegador web padrão do sistema iOS.

Analogamente às recomendações do capítulo anterior, elas impactam significativamente a usabilidade do Safari. Por isso é recomendado considerá-las como medidas de defesa em profundidade e destiná-las apenas a dispositivos iOS nos quais a segurança é primordial.

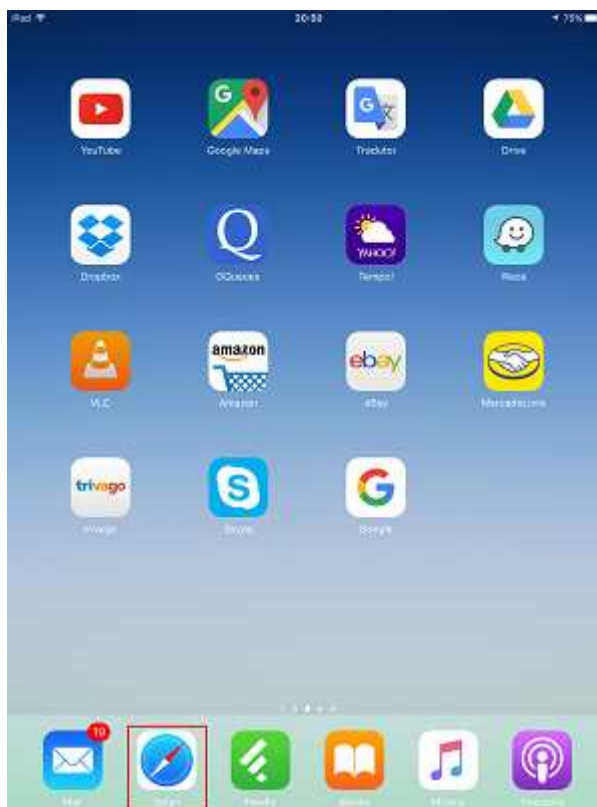


Figura 4.1: A localização padrão do ícone do navegador Safari, destacada em vermelho

## 4.1 Desabilitar a execução de código Javascript

Javascript tecnologia permite que desenvolvedores de websites controlem certos elementos de páginas web, como exibir a data e hora corrente, ou exibir janelas pop-up.

Neste item, é recomendado que a linguagem Javascript não tenha permissões de execução no navegador web padrão do dispositivo, pois a mesma pode vir a ser utilizada como meio para diversos tipos de ataques aos usuários. Tais ataques vão desde a manipulação de credenciais de login até a exibição de páginas web maliciosas, através de janelas pop-up.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Avançado
4. Desativar Javascript, deslizando controle para a esquerda

## 4.2 Habilitar o aviso de websites fraudulentos

Este controle habilita o navegador Safari a exibir avisos e impedir o carregamento da páginas de websites potencialmente fraudulentos.

Os avisos podem ajudar a evitar a visitação acidental a algum site de phishing, bem como outros sites desenvolvidos com intenções maliciosas.

1. Pressionar Ajustes
2. Pressionar Safari
3. Na seção PRIVACIDADE E SEGURANÇA, ativar Aviso de Site Fraudulento, deslizando o controle para a direita

## 4.3 Desabilitar o preenchimento automático de informações de contato

O preenchimento automático configura o navegador Safari a se lembrar de informações comumente digitadas pelo usuário em formulários na internet, para automatizar o preenchimento de formulários subsequentes.

Desabilitar o preenchimento automático ajuda a evitar o armazenamento de informações sensíveis ou confidenciais localmente no dispositivo iOS. Também reduz as chances de estas informações serem usadas de maneira não autorizada caso alguma pessoa mal intencionada obtenha acesso ao dispositivo, seja ele um iPhone ou iPad.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Preenchimento Automático
4. Desativar o preenchimento automático para Dados de Contato, deslizando o controle para a esquerda

## 4.4 Desabilitar preenchimento automático de nomes e senhas

O preenchimento automático configura o navegador Safari a se lembrar de credenciais, que geralmente são confidenciais, para automatizar o preenchimento de formulários subsequentes.

Desabilitar o preenchimento automático ajuda a evitar o armazenamento de informações sensíveis ou confidenciais localmente no dispositivo iOS. Também reduz as chances de estas informações serem usadas de maneira não autorizada caso alguma pessoa mal intencionada obtenha acesso ao dispositivo, seja ele um iPhone ou iPad.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Preenchimento Automático
4. Desativar o preenchimento automático para Nomes e Senhas, deslizando o controle para a esquerda

## 4.5 Desabilitar o preenchimento automático de cartões de crédito

O preenchimento automático configura o navegador Safari a se lembrar de números de cartões de crédito, para automatizar o preenchimento de formulários subsequentes.

Desabilitar o preenchimento automático ajuda a evitar o armazenamento de números de cartões de crédito localmente no dispositivo iOS. Também reduz as chances de estas informações serem usadas de maneira não autorizada caso alguma pessoa mal intencionada obtenha acesso ao dispositivo, seja ele um iPhone ou iPad.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Preenchimento Automático
4. Desativar o preenchimento automático para Cartões de Crédito, deslizando o controle para a esquerda

## 4.6 Apagar informações sobre senhas armazenadas

O navegador Safari fornece um repositório para armazenar informações, incluindo logins e senhas, que por sua vez dão suporte ao recurso de preenchimento automático de formulários. Senhas salvas são armazenadas no “chaveiro” do iCloud ou do dispositivo iOS, seja ele um iPhone ou iPad.

Excluir informações a respeito de credenciais salvas ajuda a impedir o uso delas, em caso de acessos não autorizados ao dispositivo.

1. Pressionar Ajustes

2. Pressionar Safari
3. Pressionar Senhas
4. Digitar o código de desbloqueio do dispositivo, caso seja necessário
5. Na tela seguinte, pressionar Editar
6. Pressionar cada credencial exibida, de modo a selecioná-las para remoção
7. Pressionar Apagar
8. Confirmar a remoção das senhas

## 4.7 Remover informações armazenadas sobre cartões de crédito

O navegador Safari fornece um repositório para armazenar informações, incluindo cartões de crédito, que por sua vez dão suporte ao recurso de preenchimento automático de formulários. Números de cartões de crédito são armazenados no “chaveiro” do iCloud ou do dispositivo iOS, seja ele um iPhone ou iPad.

Excluir informações a respeito de cartões de crédito ajuda a impedir o uso deles, em caso de acessos não autorizados ao dispositivo.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Preenchimento Automático
4. Pressionar Cartões de Crédito Salvos
5. Digitar o código de desbloqueio do dispositivo, caso seja necessário
6. Na tela seguinte, pressionar Editar
7. Pressionar cada cartão de crédito exibido, de modo a selecioná-los para remoção
8. Pressionar Apagar
9. Confirmar a remoção dos cartões de crédito

## 4.8 Habilitar a navegação privada

Habilitar a navegação privada previne o rastreamento do histórico de páginas web visitadas, pesquisas realizadas, e algumas informações utilizadas pelo preenchimento automático de formulários.

Habilitá-la pode proteger determinadas informações privadas contra uso indevido e impedir alguns sites de rastrear atividades do usuário através navegador Safari.

1. Executar o Safari
2. Pressionar o botão de abas do Safari. No iPhone ele encontra-se no canto inferior direito do Safari. No iPad ele encontra-se no canto superior direito.
3. Pressionar Privado

## 4.9 Impedir o rastreamento durante a navegação

Essa configuração instrui o navegador Safari a comunicar, para os sites aos quais ele se conecta, que não quer ser rastreado.

Tecnicamente, quando este recurso encontra-se habilitado, o navegador Safari é instruído a enviar um cabeçalho opcional em requisições HTTP realizadas a partir do navegador. Tal cabeçalho indica uma preferência de não ser rastreado por sites web; porém, ele possui natureza voluntária, ou seja, não há método ou técnica disponível para garantir que os sites web atuem em conformidade. Assim, mesmo que este recurso encontre-se configurado não existem garantias de que sites honrarão tal preferência pela privacidade.

No entanto, um grande número de sites web são sim, aderentes a esta configuração. Por isso certamente há benefícios em habilitar tal recurso.

1. Pressionar Ajustes
2. Pressionar Safari
3. Na seção PRIVACIDADE E SEGURANÇA, ativar o recurso Não Rastrear, deslizando o controle para a direita

# Apêndice A

## Referências

Neste capítulo, encontram-se listados alguns sites e livros que foram utilizados como fontes de informação para o desenvolvimento deste guia.

Cabe aqui uma ressalva sobre os endereços da internet. Mesmo tomando o máximo cuidado ao inseri-los neste capítulo, é natural que, com o tempo, eles sejam desativados ou mudem de endereço. Ou seja, alguns dos endereços utilizados correm o risco de se tornarem inválidos, ou “quebrados”. Para os leitores, sugere-se pesquisar no Google pelos endereços atuais, caso algum link abaixo esteja quebrado.

A maioria das recomendações descritas aqui foram baseadas no site de suporte da Apple, que encontra-se disponível no seguinte endereço:

<http://support.apple.com/>

O recurso Find my iPhone pode ser acessado no seguinte endereço:

<http://www.apple.com/icloud/find-my-iphone.html>

Com relação à eliminação de todas as informações armazenadas no dispositivo iOS, uma boa fonte de consulta é o livro iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices. Mais detalhes sobre este livro podem ser encontrados no seguinte endereço:

[http://textbooks.elsevier.com/web/product\\_details.aspx?isbn=9781597496599](http://textbooks.elsevier.com/web/product_details.aspx?isbn=9781597496599)

Com relação ao recurso para impedir o rastreamento durante a navegação, mais detalhes sobre a iniciativa *Do Not Track* podem ser encontrados nos seguintes sites:

- Do Not Track - Universal Web Tracking Opt Out (<http://donottrack.us/>)
- W3C Tracking Protection Working Group (<http://www.w3.org/2011/tracking-protection/>)
- Do Not Track — Electronic Frontier Foundation (<https://www.eff.org/issues/do-not-track>)